.04 Sicherheitsbedrohungen steigen weiter

Roland Kissling 22|11|2005



Fast 70 Prozent der Geschäftssysteme sind immer noch nicht ausreichend vor Angriffen geschützt. Obwohl zurzeit viele Unternehmen ihre Systeme umstellen, sind sie noch lange nicht sicher. Das besagt jedenfalls eine neue Analyse "Gesetze der Schwachstellen" des Lösungsanbieters Qualys. Die Ergebnisse basieren auf der statistischen Analyse von fast 21 Mio. kritischen Schwachstellen, die bei 32 Mio. Live-Netzwerk-Scans entdeckt wurden.

BESSER, ABER NICHT GUT GENUG

Die Ergebnisse der Untersuchung zeigen, dass die Unternehmen ihre Patching-Prozesse deutlich verbessert haben: Laut der Untersuchung benötigen Firmen durchschnittlich 19 Tage, um die Hälfte ihrer gefährdeten Internetsysteme auszubessern. Im vergangenen Jahr waren es 21 und vor zwei Jahren noch 30 Tage. "2005 war das Jahr der Verbesserungen beim Patching und Aktualisieren anfälliger Systeme", meint Gerhard Eschelbeck, CTO und VP Engineering bei Qualys. Grund dafür sei, dass viele Software-Anbieter jetzt regelmäßig Advisories mit Patch-Updates herausgäben. Das führe dazu, dass sich Unternehmen schneller um Korrekturen bemühen als bei ungeregelten Abläufen. Laut der Qualsys-Analyse verkürzt sich allerdings die Zeit von der Bekanntgabe einer Schwachstelle bis zu deren Entdeckung (Time to Exploit) bei automatisierten Angriffen weiterhin dramatisch. 85 Prozent des Schadens entsteht demnach innerhalb der ersten 15 Tage. Der Time-to-Exploit-Zyklus schrumpft also schneller als der Zyklus der Schwachstellenbeseitigung. 80 Prozent aller Exploits werden innerhalb der ersten Halbwertszeit kritischer Schwachstellen entwickelt.

WENIG GEFAHR DURCH WIRELESS?

Der Untersuchung zufolge ist die Bedrohung für drahtlose Systeme sehr gering. Nur eine von etwa 20.000 kritischen Sicherheitslücken betraf ein Wireless-Gerät. Allerdings verlagern sich die Schwachstellen zunehmend von der Server- auf die Client-Seite. Mehr als 60 Prozent aller neuen kritischen Sicherheitslücken finden sich in Kunden-Anwendungen, etwa bösartige Websites oder infizierte Mail-Anhänge.

Grundsätzlich gilt auch und gerade im Bereich der Sicherheit das Pareto-Prinzip: 90 Prozent aller Gefährdungen durch Sicherheitslücken gehen von zehn Prozent der kritischen Schwachstellen aus. Security-Experten sind also gut beraten, sich zu allererst um die wichtigsten 10 Prozent zu kümmern. (cio/kiss)